Andrew P. Bridges (SBN 122761)
Jennifer Golinveaux (SBN 203056)
K. Joon Oh (SBN 246142)
Thomas J. Kearney (SBN 267087)
WINSTON & STRAWN LLP
101 California Street
San Francisco, CA 94111-5802
Telephone: (415) 591-1000
Facsimile: (415) 591-1400

Attorneys for Defendants
GIGANEWS, INC. and LIVEWIRE SERVICES, INC.

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

PERFECT 10, INC., a California corporation,

Plaintiff,

vs.

GIGANEWS, INC., a Texas corporation; LIVEWIRE SERVICES, INC., a Nevada corporation; and DOES 1 through 100, inclusive,

Defendants.

Case No. 11-CV-0905 H (MDD)

EXPERT DECLARATION OF WILLIAM R. ROSENBLATT IN SUPPORT OF DEFENDANTS' OPPOSITION TO MOTION FOR PRELIMINARY INJUNCTION

Special Briefing Schedule Ordered

DATE: September 12, 2011
TIME: 10:30 a.m.
CTRM: 13
JUDGE: Marilyn L. Huff

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

I, William R. (Bill) Rosenblatt, declare as follows:

A. Introduction and Qualifications

1. I have been asked to express a professional opinion on technical issues related to Plaintiff's allegations of copyright infringement and motion for preliminary injunction in this matter, and specifically with respect to the feasibility of filtering or other content management tools to detect infringement in Usenet servers. Except where otherwise stated, I have direct and personal knowledge of the facts set forth herein and, if called as a witness, can and will competently testify thereto.

2. I am president of GiantSteps Media Technology Strategies, a consultancy that I formed in June 2000. GiantSteps consults on technology strategy related to digital content with

particular emphasis on digital rights technologies, digital content management, and the Internet.

3. My involvement in these fields dates back to 1994, when I was Director of Publishing Systems at Times Mirror Co., then a diversified publishing company with $3 billion in annual revenues. I was appointed to represent the company on a publishing industry committee tasked with developing pro-competitive standards to address the emerging issue of online copyright management. I was one of the designers of the standard that came out of this initiative, the Digital Object Identifier (DOI). The DOI is widely used today in academic and scientific publishing.

4. As a consultant, my clients have included companies from across the spectrum of digital rights and online content issues, including technology companies (ranging from early-stage startups to companies like Microsoft, IBM, and HP), network service providers (including telephone and cable providers), and copyright owners (including major film studios, record labels, and various types of publishers). I have consulted to several companies on subject matter related to content recognition and identification.

5. I have also testified before, or provided consulting to, public entities including the Copyright Office, Federal Trade Commission, National Academies, and European Commission, as well as advocacy groups such as the Business Software Alliance and Association of American Publishers.

6. I am the author of *Digital Rights Management: Business and Technology* (Wiley, 2001), the chapter "Digital Rights and Digital Television" in *Television Goes Digital* (Springer, 2010), and several white papers and articles on digital rights and online content, including the white paper *Content Identification Technologies: Business Benefits for Content Owners* (2008). I was editor of the online newsletter DRM Watch from 2001-2009, which is now the blog Copyright and Technology.

7. I have chaired the Digital Rights Strategies and Copyright and Technology conferences from 2004 to the present. I have spoken on related subject matter at conferences on five continents, including the World Economic Forum (Davos); Congressional Internet Caucus State of the Net; National Association of Broadcasters; Progress and Freedom Foundation Aspen Summit; European Union Online Content for Creativity; ACM Computers, Freedom, and Privacy, Asian

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

Festival of Children's Content; and various others. I have guest lectured on digital copyright at several colleges and law schools. I have been quoted on related subject matter in publications in eight countries including *The New York Times, The Guardian, Der Spiegel, Billboard*, and various trade publications.

8. My familiarity with Usenet dates back to 1985, when I was employed as a Unix system administrator at Intermetrics Inc. (now L3 Communications) and used it routinely in my work. Intermetrics did software development work for government and defense clients and thus had access to ARPANET, a precursor to the Internet. Usenet ran on ARPANET before the Internet existed (see ¶16).

9. The fundamental software components of the Internet were all built on and for Unix-based computer systems. This includes Usenet and all of the communications protocols on which it depends; see ¶21-22 below. My expertise in Unix systems led to my authorship of two books on Unix-related subjects published by O'Reilly & Associates in the early 1990s, as well as publication of various articles on Unix-related topics for periodicals such as *UnixWorld, SunWorld,* and *SuperUser* (the latter being a synonym for system administrator).

10. My educational background includes a B.S.E. in Electrical Engineering and Computer Science, *cum laude*, from Princeton University (1983), an M.S. in Computer and Information Science from the University of Massachusetts (1990), and PhD coursework and research at UMass in programming languages, databases, and software engineering.

11. I served as a software engineer at Motorola and Intermetrics (see above) between college and graduate school. I have written software in several programming languages for a total of over ten years. Attached as Exhibit F is a copy of my curriculum vitae.

B. Summary of Opinions

12. The following are summaries of the opinions expressed herein:

- Plaintiff's documents in support of their motion for preliminary injunction contain various misunderstandings, false assertions, and misrepresentations. ¶31 and onwards.
- Usenet message headers do not necessarily indicate the content in message bodies, as Plaintiff claims they do. ¶32-37.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

- "Image Identifiers," a term invented by Plaintiff, are not unique IDs for Usenet messages or the content therein. Only Message-IDs are unique IDs for Usenet messages. ¶38-41.
- The "image recognition" (content identification) technologies that Plaintiff suggests Defendants use are unworkable. ¶42-61.
- Defendants' demands for message headers and Message-IDs are proper and reasonable for notices pursuant to 17 U.S.C. § 512(c). ¶62-70.

13. Before I explain my opinions, I provide some background on Usenet, the Internet, and the World Wide Web that may help frame the issues in this litigation.

C. Background on Usenet, the Internet, and the Web

14. Here I provide some historical and technical background on the Internet, Usenet, and the World Wide Web in order to draw attention to the differences among them that are relevant in considering the issues raised in this litigation.

15. Usenet is a set of communications protocols and tools for using them. In general, a protocol is a machine-readable language for communicating among different systems on a network. Digital networks like the Internet depend on layers of protocols, from the physical layer, involving bits and bytes sent over communication links, all the way up to protocols that support end-user applications, which are programs that users see and interact with on their computers.

16. Usenet was invented in 1979 by two graduate students at Duke University[1]. The Internet as we know it today did not exist back then; Usenet ran on government computer networks based on variants of the fundamental IP (Internet Protocol), such as the ARPANET.

17. The Internet is generally considered to have come into being in 1988[2]. The first commercial Internet service providers (ISPs) started a year thereafter.

18. The World Wide Web (or simply the "web" as it is commonly known today) was invented in the late 1980s by Tim Berners-Lee at CERN labs in Switzerland. Berners-Lee created

[1] See for example C. Lueg and D. Fisher, *From Usenet to CoWebs: Interacting with Social Information Spaces* (Springer, 2003).
[2] See for example V. Cerf and B. Aboba, *How the Internet Came to Be* (1993). Available at http://www.netvalley.com/archives/mirrors/cerf-how-inet.html.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

the first web browser, WorldWideWeb, in 1990 and made it publicly available in 1991[3]. However, WorldWideWeb only ran on NeXT workstation computers. The browsers that we use today can all trace their origins to the MOSAIC browser built at the University of Illinois in 1993[4].

19. The web has two essential building blocks: the communications protocol HTTP (HyperText Transfer Protocol) and the file format HTML (HyperText Markup Language). HTML is a language for adding formatting instructions (bold, italics, font size, headings, paragraphs, numbered lists, etc.) to text; it is also used for adding *hyperlinks*, which are links to other HTML pages that a user can click on to go to other web pages. HTTP is a method of, among other things, retrieving HTML pages from other computers connected to the Internet when a user clicks on a hyperlink.

20. A website is an interlinked collection of HTML pages, usually tied to a principal page called a "home page" such as http://www.casd.uscourts.gov/.

21. In contrast, Usenet is currently based on a much earlier and very different communications protocol called NNTP (Network News Transfer Protocol), invented in 1986[5] and based on the even earlier SMTP (Simple Mail Transfer Protocol) for e-mail. NNTP replaced the original UUCP (Unix-to-Unix Copy) protocol used in Usenet which was first released in 1979.

22. HTTP and NNTP are both protocols that depend on the fundamental low-level protocols of the Internet, such as Internet Protocol (IP), but otherwise they are separate and distinct, just as email is distinct from web pages. As can be seen from the above, Usenet predates the web by over a decade.

23. Users interact with the web using *web browsers* such as Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome; Users interact with Usenet using *newsreaders* such as News Rover (S&H Computer Systems) or NewsShark (WMHSOFT). Many different newsreaders are available today[6]. Newsreader functionality is also built into some email programs, such as Microsoft Outlook Express.

---

[3] http://www.w3.org/People/Berners-Lee/WorldWideWeb.
[4] http://totic.org/nscp/demodoc/demo.html.
[5] http://tools.ietf.org/html/rfc977 .
[6] See for example http://www.newsreaders.info/recommended-newsreaders.htm.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

24. There are many important architectural differences between the web and Usenet. Many of these result from the very different sets of assumptions about computers and networking capabilities that existed in 1979 (Usenet) vs. the early 1990s (the web).

25. On the web, entities (companies, individuals, institutions, etc.) maintain websites, which (as mentioned above) are collections of web pages. Web pages are identified by URLs (Uniform Resource Locators) such as https://www.giganews.com/signup/ or http://www.perfect10.com/join.html. *URLs are globally unique IDs of locations of particular resources on the web:* they refer both to a server at a general level and to file paths and files on that server at a more particular level. For example, if a user types "http://www.casd.uscourts.gov/uploads/Rules/General Orders/GO_596.pdf" into a web browser, that directs the browser to retrieve the resource "Rules/General Orders/GO_596.pdf" (a document in Portable Document Format (PDF)) on the server www.casd.uscourts.gov.

26. The entity operating the website uploads HTML pages to the site by saving the page on a server associated with the site. Users access web pages by typing URLs into their web browsers or clicking on hyperlinks on web pages or other documents. In either case, the browser invokes the HTTP protocol to retrieve the requested web page from the website in question. Under normal circumstances, the web pages on a given website are *only directly available from that website*, not from any other sources. Of course, virtually identical pages may exist elsewhere, with different unique URLs, but any URL only points to a single location.

27. In contrast, the architecture of Usenet is based on multiple repositories of *messages.* Users, not Usenet service operators, post messages to Usenet servers. Messages are copied from one Usenet server to another via NNTP. Usenet servers *propagate messages to other Usenet servers* so that all Usenet servers are up to date. This propagating, message-passing architecture arose in the milieu of the late 1970s to early1980s with slow network connections and the lack of a system that automatically figured out how to route a request from a server through other servers on the network to the user's computer[7].

[7] The system, DNS (Domain Name System), was invented in 1983. It specifies *domain names* like yahoo.com and google.com that we take for granted today. Before DNS, users had to know and specify all of the servers in a route (pathway) between the server from which they requested

28. The format of a Usenet message is very different from the format of a web page (HTML). The Usenet message format is specified in an IETF (Internet Engineering Task Force) specification designated RFC 1036[8]. Usenet messages contain *headers* consisting of *fields*, some required, some optional. The required fields are:

- **From**: the claimed email address of message poster.
- **Date**: date of original posting.
- **Newsgroups**: newsgroups to which the message has been posted. A description of newsgroups is reproduced in Exhibit A from the reference book *The TCP/IP Guide*[9].
- **Subject**: similar to the subject line in an email message.
- **Message-ID**: identifier for the message. *Message-IDs are globally unique on Usenet*[10]. Message-IDs can be reused, but no more than one message with a given Message-ID must be in existence on Usenet at any given time. Messages are retained on servers according to the service provider's retention policy, which is the length of time that the service provider keeps messages.
- **Path**: list of systems through which the message passed to get to the server on which the user is reading the message. A message's path will differ for the same message on two different service providers.

After the headers comes the body of the message, which can consist of text or any other data. Message body data that is not text is encoded in a text format, in order to signal "here comes some non-text content" to the software and to ensure that the message remains intact in transit from one Usenet server to another. E-mail uses a similar technique for encoding files attached to messages, e.g. Microsoft Word documents or users' digital camera pictures.

29. Usenet service providers such as Defendants do not store searchable indexes of message bodies. A Usenet service provider would have to build a separate index for searching message bodies, akin to the index that a search engine for web pages such as Google maintains. This is not a standard feature of Usenet servers, nor do I understand that Giganews has implemented such

---

information and their own computers.

[8] http://www.ietf.org/rfc/rfc1036.txt.

[9] C. M. Kozierok, *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* San Francisco: No Starch Press, 2005, pp. 1404-6.

[10] "The article's message ID is a fixed identifier that can be used to uniquely represent it across Usenet[.]" Kozierok, p. 1417. "The "Message-ID" line gives the message a unique identifier. The Message-ID may not be reused during the lifetime of any previous message with the same Message-ID." http://www.ietf.org/rfc/rfc1036.txt, Section 2.1.5.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

a feature.

30. Table 1 below summarizes the most important differences between the web and Usenet for purposes of analyzing issues relevant to this dispute.

	Usenet	Web
Invented	1979	1990-1993
Application protocol	NNTP	HTTP
Content type	Message with header	Web page
Content format	RFC 1036	HTML
Unique content identifier	Message-ID	URL
Server architecture	Propagated: users post messages to servers, which distribute them to other service providers; users can retrieve posts from any provider with the post	Single server: website administrators upload pages to servers; users must retrieve pages only from those servers.

Table 1: Key differences between Usenet and the web.

D. Misunderstandings in Perfect 10's Motion for Preliminary Injunction

31. I have read Plaintiff Perfect 10, Inc.'s Memorandum of Points and Authorities in Support of Its Motion for Preliminary Injunction Against Defendants Giganews, Inc. and Livewire Services, Inc. (hereinafter "PI Memo"). I have also read Declaration of Dr. Norman Zada in Support of Plaintiff Perfect 10, Inc.'s Motion for Preliminary Injunction against Defendants Giganews, Inc. and Livewire Services, Inc. (hereinafter "Zada Decl.") and Declaration of Sean Chumura in Support of Perfect 10's Motion for Preliminary Injunction against Defendants Giganews, Inc. and Livewire Services, Inc. (hereinafter "Chumura Decl."). These documents contain a number of misunderstandings, false assertions, and misrepresentations that materially impair the validity of the conclusions Plaintiff draws.

E. Usenet Message Headers Do Not Necessarily Indicate the Content in Message Bodies.

32. A major area of misunderstanding in the PI memo concerns a Usenet server's ability to enable search for content of Usenet messages. As mentioned above at ¶29, Giganews does not index the actual content of messages for search. It is true that Usenet messages may contain binary file attachments in their message bodies (just as email messages can contain file attachments) and

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

that those messages' Subject headers might contain the names of those files. Yet Plaintiff's arguments rely heavily on the assumption that Subject fields accurately identify content in message bodies. This assumption does not always hold true.

33. The lack of correspondence between Subject fields and content works both ways: some filenames in Subject fields claim to identify content that turns out not to be the presumed content, and some filenames are altered or obfuscated in order to evade detection.

34. Here are examples of both of these occurrences:

35. **Decoy or spoof files**: So-called antipiracy service providers routinely upload decoy files with filenames suggesting copyrighted content, intended to attract users who intend to download them. When the user downloads such a file and tries to view or play it, he sees or hears something that he didn't expect, such as noise[11]. Examples of antipiracy service providers that perform this service include BayTSP Inc. and MediaDefender Inc. These companies provide their services on different parts of the Internet, including Usenet[12]. These companies keep their clients' identities confidential, but it is publicly known that major brand-name content providers pay to engage their services[13].

36. **Disguised malware**: another use for deceptive Subject fields is as "honey pots" for malware, such as spyware, adware, viruses, etc. Users download the messages and detach the files, thinking that they are content described in the Subject field, but they turn out to be malware that installs itself on users' computers and shows unwanted ads, reports users' activities to a server without permission, etc.[14]. Popular entertainment content titles[15] are commonly used for this purpose. This technique is used on Usenet[16] as well as other Internet services.

---

[11] See for example http://www.mediadefender.com/antipiracy.html.
[12] See for example http://www.baytsp.com/services/tracking.html
[13] Leaked e-mails reveal MediaDefender's antipiracy woes. CNet News.com, September 20, 2007. Available at http://news.cnet.com/Leaked-e-mails-reveal-MediaDefenders-antipiracy-woes/2100-1027_3-6209084.html?tag=st.prev
[14] "Spyware that causes . . . problems can also be hidden in downloaded 'shared' files." *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues.* Staff Report, Federal Trade Commission, June 2005, p. 9. Available at http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf.
[15] See for example http://www.net-security.org/malware_news.php?id=1005.
[16] See for example http://filesharingtalk.com/threads/346665-.exe-files-in-usenet, http://forums.whirlpool.net.au/archive/1338461, http://www.royhochstenbach.nl/new-malware-hiding-trick-on-usenet-discovered/, http://www.pcreview.co.uk/forums/beware-new-circulating-

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

37. **Name obfuscation**: Some users may post copyrighted materials and obfuscate (disguise) filenames in ways known to other users, in order to evade detection. For example, users give filenames in Subject headers obfuscated names designed to fool search algorithms but attract knowledgeable users. A common technique for this is known as "Leet" or "Leetspeak."[17]. Leet is a set of orthographical transformations, such as substituting numerals for letters (e.g. 0 for O, 1 for L, 3 for E; in fact "1337" is Leet for "Leet"), punctuation characters for letters (e.g. @ for a, $ for s), punctuation characters or numerals for phonemes (& for "and," 2 for "to" or "too"), phonetic substitutions ("z" for "s" at the end of plural nouns such as "warez,") etc. "P0rn" or "pr0n" are often-used Leet words for "porn"[18]. Leet is used all over the Internet, including in ubiquitous emails with subject lines including "vi@gr@" and "ch3@p drug$," intended to evade spam filters but to be understandable to the general public, and also to obfuscate the names of files that may contain objectionable material[19].

F. "Image Identifiers" Are Not Unique IDs for Usenet Messages.

38. Another major area of misunderstanding is Plaintiff's underlying assertions that what it calls "Image Identifiers" constitute unique content identifiers for Usenet. This is not the case. Plaintiff has invented the term "Image Identifier" to create the impression that there is such a thing on Usenet: ". . . **what I refer to** as the 'Image Identifier.'" (Zada Decl. ¶7, emphasis added); "Each image displayed an Image Identifier, such as, me915@P10-Karolina_Runosson_004. JPG, which identified the specific file on Defendants' servers" (PI Memo p. 9 at 7-9). There is no such standard term, neither in the RFC 1036 Usenet message format specification nor in common Usenet parlance.

39. Indeed, searches of Usenet indicate that what appears to be the same intellectual property is posted by users who give it different Subject field values. An example of this is shown in Exhibit B, which shows the results of a Usenet search, using the News Rover newsreader, for Zoya Konyieva, a model whose images Plaintiff claims to own or license (see for example Zada Decl. Exh. 3 p. 1). The screenshot, which was taken July 26, 2011, shows seven search results. As is

usenet-malware-cryptosms-exe-t2291084.html.

[17] See for example http://www.technewsworld.com/story/47607.html.

[18] Ibid.

[19] http://people.uwec.edu/greener/TermPapers2/ChrisCortner-FinalRev-4-05-09.pdf.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

evident, there is no common scheme that would suggest an "image identifier" in these Subject header fields.

40. As mentioned above in Table 1 (¶30) among other places, Message-IDs are the only guaranteed unique identifiers of content on Usenet.

41. Furthermore, Subject fields are neither designed nor guaranteed to be unambiguous as locators of files attached to messages on Usenet. For example, Exhibit C shows the results of a Usenet search for "Ubuntu Oneiric Ocelot," a distribution of the open-source Linux operating system[20], on August 9, 2011. As the screenshot shows, there are many messages with exact duplicate Subject fields in the search results; yet for each set of messages with identical Subject fields, the size in kilobytes (K bytes) of each message is different, meaning that each message contains different content. For example, Exhibit C shows three messages with Subject fields "[Multi] Ubuntu 11.10 (Oneiric Ocelot) Alpha 1.rar," each with different message sizes. In fact, duplicate Subject fields are so common that the News Rover newsreader has an "eliminate duplicate entries" option.

G. Content Identification Technologies Cited by Plaintiff Are Unworkable.

42. Plaintiff expects Defendants to use "readily available image recognition software to block [infringing] images" (PI Memo, p. 10 at 2-3). In the field of rights technologies, the term "content identification"[21] is preferred to "image recognition," so I use it here.

43. Dr. Zada proffers various flavors of content identification and filtering solutions in his Declaration. In all cases, using such techniques would be unduly onerous to Usenet service providers such as Defendants. In addition to the computational tasks required for each of them, as described below, it would be necessary to decode *every binary file on the server* from its text encoding (see ¶28) in order to examine its contents. This task is not only computationally significant by itself in a Usenet context but is also not required of similar operations on websites, where files are

[20] "Distributions," or "distros" for short, are sets of software that are derived from the original Linux open-source operating system but with different enhancements or configurations. The Ubuntu distro uses adjective-animal alliterations in lieu of version numbers; thus "Oneiric Ocelot" succeeds "Natty Narwhal," which in turn succeeded "Maverick Meerkat."

[21] See for example B. Rosenblatt, *Content Identification Technologies: Business Benefits for Content Owners*. GiantSteps Media Technology Strategies white paper, available at http://www.giantstepsmts.com/Content%20ID%20Whitepaper.pdf.

stored in their native formats without text encoding.

44. All of the techniques proffered by Dr. Zada would require expenses of acquiring and running such software. They would also generally slow down performance and therefore unfairly hobble Defendants with a usage disadvantage relative to their competitors, and/or require Defendants to spend more money on infrastructure to make up for the loss in performance. Furthermore, because of the propagating architecture of Usenet (see above at ¶23 and Table 1 at ¶30), it would also unfairly single out Giganews for content filtering compared to other Usenet servers, *many of which host the same content, and some of which supply it to Giganews on a regular basis*. Note that the latter is not the case on the web, where there is no inherent mechanism for propagating content of a single website to other websites.

45. In addition, none of the techniques mentioned by Dr. Zada would be sufficiently effective to both remove Plaintiff's claimed content and eliminate the likelihood of false positives, i.e. unfairly block content that has nothing to do with Plaintiff.

46. Now I will turn to the specific content identification techniques proffered by Plaintiff. "[Defendants] could simply use an image recognition program to scan their servers and remove any image that displays a Perfect 10 copyright notice." (Zada Decl. ¶31.) This technique would not be effective, as it is trivial to remove a copyright notice from a digital image before posting it to Usenet, even if the copyright notice is superimposed on the image, and even though removal of copyright notices is a violation of 17 U.S.C. § 506(d). Moreover, Plaintiff does not superimpose copyright notices on at least some of their images; see for example Zada Decl. Exh. 14 p. 4-6. Even if this technique were imposed, it would be a minor deterrent to would-be infringers: they would simply hide or manipulate the copyright notice so that the OCR (optical character recognition) would not recognize the text. It would be a simple matter to make a tool freely available that does this, so that users who want to post images can easily use it without any technical savvy. Such a tool could work on any digital image.

47. The tactic of distributing an easy-to-use tool that helps users evade copyright protection is not merely hypothetical; it has rich precedent. For example, so-called "DeCSS rippers" for decrypting protected DVD content were commonly available after the encryption scheme for

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

DVDs was hacked in 1999[22]. Even though the courts found that such a scheme was a violation of copyright law under 17 U.S.C. § 1201[23], DeCSS rippers have remained widely available[24]. Like the copyright notice hiding tool described above, DeCSS rippers are usable without special technical skill and work on content from any protected DVD in the world.

48. In other words, the proffered technique of searching for Plaintiff's copyright notices would not be very effective in stopping any copyright infringement, while still creating a significant burden for Defendants.

49. "Defendants could work with Perfect 10, who could provide them with [a] disk of Perfect 10 Images. Defendants could then scan their servers and remove any images which matched any of those on the disk." (Zada Decl. ¶31.) This technique is especially onerous to implement for the technical reasons described above at ¶43. Furthermore, the term "match" is problematic in this context. I assume that Dr. Zada means "exact match," since he distinguishes this technique from fingerprinting techniques, which are based on inexact matches (see below at ¶54). It is even easier to foil an exact-match search than it is to hide copyright notices. All that is necessary is to change a couple of bits in the digital image file (a technique known as "bit-twiddling"); then the match would fail. In fact, many images that users posted to Usenet are probably changed from the originals in some way, whether on purpose or by happenstance, via format conversion, resizing, color shift, scanning, etc. None of these images would match either. Otherwise, a simple utility could be created that twiddles bits in digital content files so that they can be posted online and escape detection by exact-match algorithms – in the same vein as the copyright notice removal tool discussed above. In fact, the ineffectiveness of this matching technique is probably the main reason why it is not used anywhere for purposes such as Plaintiff has in mind[25].

---

[22] See for example: Free Speech Rights for Computer Code?. *The New York Times*, July 31, 2000. Available at http://www.nytimes.com/library/tech/00/07/biztech/articles/31rite.html.

[23] Among others, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), aff'd, 273 F.3d 429 (2d Cir. 2001).

[24] See for example http://decss.zoy.org/ or http://www.cs.cmu.edu/~dst/DeCSS/Gallery.

[25] See for example http://w2.eff.org/share/audible_magic.html for an explanation of the difference between fingerprinting and simple hash algorithms; the latter are efficient ways to compute exact matches as described herein (see ¶55): "[The fingerprinting] method is a clear improvement over earlier 'hash'-based filtering approaches. With those earlier approaches, changing even a single bit in a file would frustrate efforts to match the file to a pre-calculated hash. "

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

50. Dr. Zada suggests the use of "find similar images" techniques such as those of Google and Microsoft's web search engines (Zada Decl. ¶31). First of all, these techniques are designed for use on the web, not Usenet; they depend on search engines' continuously-maintained indexes of images and associated data (e.g., captions) throughout the web. They would need to be radically re-architected to work on Usenet, which includes having to decode each file attachment (see ¶43) before each image could be examined. But even if this were feasible, these techniques were not designed for the use that Plaintiff have in mind. They would introduce an overwhelming number of false positives. Exhibit D illustrates this. The first screenshot (Figure 1) shows results of a Google image search on "Zoya Konyieva" (see ¶39 above) with the computer's mouse over one of the images to show the "Similar" link. The second screenshot (Figure 2) shows the result after clicking on "Similar": two images that are obviously not the same. Thus, this technique identified two of the many images of Zoya Konyieva as "similar." The second image would be "collateral damage" if Defendants used this technique to remove images from its servers, because (among other reasons) there is no guarantee that the second image is the intellectual property of the claimant. Also note that this technique did not identify *all of the images of the same person* as "similar," nor did it identify *only truly identical images* as "similar." Thus the technique is not very effective for Plaintiff's purposes. It is intended to be a handy search tool for end-users, not a way of definitively identifying content for any purpose.

51. The same experiment done with the analogous feature in Microsoft's Bing search engine produced many more false positives, as shown in Exhibit D Figure 3 and Figure 4. Just as with Google as described above, the first screenshot shows results of a Bing image search on "Zoya Konyieva" with the mouse over one of the images to show the "Similar images" link. The second screenshot shows many "similar" pictures – 71 to be exact – some of which do not even look like the same person, such as the image circled in Figure 4.

52. In fact, the issue of false positives appears to be one that Plaintiff is aware of and appearing to obscure. The examples that Dr. Zada used for Google and Microsoft "similar image" search appear contrived to show no false positives, and they are not representative of the actual ability of the technology. Zada Decl. Exh. 24 p. 3, for example, purports to show a Google image

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

search for "Anjelina [sic] Jolie" on blogspot.com, which is the domain name for Google's popular Blogger service. Notice the line at the top that says "Back to results for site:blogspot.com 'Anjelina Jolie'." This suggests that Dr. Zada selected a specific image from those search results such that, when he clicked on "Similar," many copies of the same image (i.e. no false positives) would come up. In other words, this appears to be an intentionally anomalous result. To test this, I ran the identical Google image search of "site:blogspot.com 'Anjelina Jolie'" on July 26, 2011, the results of which are shown in Exhibit D Figure 5 and Figure 6 and are completely different from the results in Zada Decl. Exh. 24. The results of clicking on "Similar," shown in Figure 6, show several different images of Angelina Jolie, in which many different entities could hold copyright.

53. A Microsoft Bing image search that I ran on the same date for "Marisa Miller" (the search shown in Zada Decl. Exh. 24 p. 5) similarly shows that Dr. Zada's example appears contrived to show no false positives. Once again, I ran the identical search, with the results (Exhibit D Figure 7 and Figure 8) being very different from Dr. Zada's and showing many false positives.

54. Dr. Zada then suggests using services such as TinEye and Attributor (Zada Decl. ¶31). These services use variations on a technique known as *fingerprinting*. Dr. Zada quotes TinEye's description of fingerprinting, which is accurate as far as it goes, if somewhat incomplete. The term "fingerprinting" analogizes the notion of taking a criminal suspect's fingerprints and looking them up in a database of known fingerprints. In this case, the "fingerprint" is a number (or set of numbers) that an algorithm calculates from the bits in a content file, which represent the content itself.

55. In mathematical terms, a fingerprinting algorithm is a variant of a *hash* algorithm. A hash algorithm is like a mathematical funnel: a large amount of data goes in; a very small amount of data comes out. A hash is a compact representation of data such that if the data changes, the resulting hash value changes, and different inputs are extremely unlikely to produce the same hash values. A common use of hashes is in data communications, to ensure that data transmitted to another location arrives intact: the hash value is calculated at the transmitting end and sent along with the data. The receiver receives the data and re-calculates the hash. If it is the same as the hash sent along with the data, then the data has arrived without being altered.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

56. The problem with standard hashing algorithms in finding matches to digital content is that it is trivially easy to modify the content so as to fool the hash algorithm, using the same bit-twiddling technique as described above at ¶49. In fact, the most common uses of hashing (such as in data communications) are intended specifically to catch changes to one or two bits of the data. Therefore, more sophisticated variations of hash algorithms have been developed that make allowances for changes to the content that do not affect human perception of it, including (in the case of still images) resizing, cropping, format conversion, color shifts, scanning, and so on. These are known as fingerprinting algorithms[26]. Fingerprinting algorithms exist for text, audio (music), and video as well as for still images.

57. Dr. Zada mentions Attributor and TinEye (Idée Inc.) as examples of fingerprinting service providers for still images. These services have indeed been used to find allegedly infringing content. However, neither TinEye nor Attributor is usable on Usenet. Their technologies are based on crawling the web for images and comparing them with images submitted by customers: "TinEye regularly **crawls the web** for new images" (http://www.tineye.com/about, emphasis added); "[Attributor's] solution combines superior **web crawling** technology with a trained professional services team" (http://www.attributor.com/products/guardian, emphasis added). Dr. Zada did not cover this aspect of these companies' technologies in his Declaration. Both companies (and others like them, such as PicScout) would have to radically re-architect their solutions to work on Usenet servers, as is the case with search engines' "find similar images" techniques (see ¶50 above).

58. Furthermore, these services work on behalf of content owners, not Internet service providers. For example, Idée's customers for its PixID image monitoring service (a paid subscription service from Idée based on the same technology as TinEye) include news wire services such as Associated Press and Agence France-Presse; whereas Attributor is primarily involved in fingerprinting of text content at the behest of news, book, and magazine publishers[27].

59. Even if these services could be re-architected to work on Usenet, it would be

[26] They are also known among researchers as "robust hashing" or "perceptual hashing" algorithms.
[27] http://www.attributor.com/company/about-us lists Macmillan, Harper Collins, John Wiley & Sons, the Associated Press, Financial Times, Agence France-Presse, and the Spanish news agency EFE as customers.

unreasonably burdensome for Defendants to operate them on content owners' behalf, for reasons described above at ¶42.

60. Finally, Plaintiff asserts that Defendants' "failure to adopt relatively simple means of reducing infringement through keyword filtering is evidence of Defendants' culpability." (PI Memo, p. 16 at 19-20.) I assume that Plaintiff's reference to "keyword filtering" means blocking messages whose header fields, including Subject fields, contain one or more terms from a designated list of terms (keywords). Such a technique would produce many false positives, just as the "find similar images" techniques described above (¶50-53). For example:

- Filtering on any of the names of models whose images Plaintiff claims to own or license would result in false positives in the manner of the "find similar images" technique described above.
- Filtering on "P10," a claimed trademark of Plaintiff (see PI Memo, p. 9 at 25-26), would also block many files that have nothing to do with Plaintiff. The results of a search on July 25, 2011 on "P10" – limited to messages with file attachments – are shown in Exhibit E. As the screenshot shows, there are several messages such as the first result, "Half Blood Blues **P10**, Book at Bedtime 110708 160k.mp3 yEnc" (an audio file), and "10 Flash Template Website K25 **P10**.exe" (an executable program) (emphasis added to show matching search terms), that have nothing to do with Plaintiff.

61. Thus none of the content identification or image recognition techniques proffered by Dr. Zada in his Declaration are workable for Defendants.

H. Defendants' Demand for Message Headers or Message-IDs in DMCA Takedown Notice Requirements Are Proper and Reasonable.

62. Plaintiff's arguments rest on the notion that Defendants should respond to takedown notices under 17 U.S.C. § 512(c) when such notices contain "Image Identifiers," which (as explained above, see ¶38) is not a Usenet term of art but a term invented by Plaintiff that actually describes Subject fields in Usenet message headers. Proper takedown notices must include information enumerated in 17 U.S.C. § 512(c)(3)(A). In my opinion, Subject fields fail to meet this standard for at least the following reasons:

- Subject fields do not qualify as "[i]dentification of the copyrighted work claimed to have been infringed" (17 U.S.C. § 512(c)(3)(A)(ii)). Only Message-IDs can reliably identify messages on Usenet (see ¶38-41), which is why Defendants properly require

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

them in takedown notices to which they can legitimately respond[28]. Furthermore, Subject fields do not necessarily identify content accurately, as explained above (see ¶32-37).

- Subject fields do not qualify as "information reasonably sufficient to permit the service provider to locate the material" (17 U.S.C. § 512(c)(3)(A)(iii)). Subject fields are not unambiguous as identifiers of content (see ¶41).

63. Plaintiff claims that using Message-IDs to identify content in takedown notices is "unworkable" (PI Memo p. 10 at 17) and provide several reasons, all of which are specious:

64. "Defendants could have searched their servers using a particular Image Identifier to find every article offering that same image." (PI Memo p. 9 at 17-18.) See above at ¶39 as to why this technique would not be effective; see above at ¶41 as to why Subject fields are not unique identifiers.

65. "[T]he Image Identifier normally contains the name of the model, [e.g.], Karolina Runosson. By searching on the model's name, Defendants could have found multiple infringing P10 Images of that model in one search." (PI Memo p. 9 at 21-24.) This is incorrect; see above at ¶35-36 regarding spoofs and decoys. Furthermore, results of such a search may include messages containing content not owned or licensed by Plaintiff.

66. "[T]he Image Identifier me915@P10-Karolina_Runosson_004.JPG, contains one of Perfect 10's claimed trademarks, 'P10,' which Defendants could have searched on as well to immediately find and remove **thousands** of articles containing P10 Images." (PI Memo p. 9 at 24-27, emphasis in original.) This is also incorrect. Doing so would remove many files that have nothing to do with Plaintiffs; see above at ¶60. It would be unduly burdensome and restrictive to require Defendants to remove such files at the behest of a party that does not hold copyright in such files.

67. "[B]ecause Perfect 10 provided copies of the infringing images, Defendants could have used readily available image recognition software to block such images from ever reappearing on Defendants' servers." See above, Section G (¶42-61), for discussion of the infeasibility of this type of technology for this application.

[28] http://www.giganews.com/legal/dmca.html.

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

68. "[W]hat Giganews requires (the Message ID) is a string of incomprehensible characters such as 1eidnavRr6r3HTbQnZ2dnUVZ_s0AAAAA@giganews.com" (PI Memo p. 10 at 5-7). The fact that the Message-ID is not mnemonic is immaterial. Unique content identifiers are not required to be mnemonic; they are required primarily to be machine readable. Examples of such content identifiers abound, including DOIs (see ¶3 above) and International Standard Book Numbers (ISBNs) for books. Many Internet service operators have responded to takedown notices under 17 U.S.C. § 512(c) that include, for example, non-mnemonic web URLs. For example, a video of Lady Gaga's "Born This Way" on YouTube has the URL http://www.youtube.com/watch?v=wV1FrqwZyKw&ob=av2e.

69. "[I]t takes approximately 45 seconds to locate, verify, and accurately cut and paste each Message-ID into a spreadsheet. Thus, to provide the Message-IDs for the 46,000 P10 Images that Giganews is currently infringing, **would take over three months**." (PI Memo p. 10 at 13-16, emphasis in original.) To support this assertion, the PI Memo cites declarations including that of Sean Chumura, which states: "[T]he copyright holder would have to manually cut and paste the message-ID in to a spreadsheet, which would take weeks if thousands of images were infringed." (Chumura Decl. p. 6 at 21-23.) This is untrue. It is not necessary to "manually cut and paste" Message-IDs into a spreadsheet or other document used to produce proper takedown notices. Instead, one could write a program that uses the NNTP protocol to retrieve Usenet messages, extract the Message-ID from each, and insert it into a file of identifiers of allegedly infringing messages. In fact, Mr. Chumura admits that he wrote a similar program: "I have written a program for Perfect 10 which automatically downloaded images from USENET paysites." (Chumura Decl., p. 2 at 5-6.) Any such program would have to use NNTP commands such as ARTICLE to retrieve (download) messages that may contain digital images. The ARTICLE command retrieves a message, including the header, which in turn includes the required Message-ID field. Thus it would be trivial to modify any such program to read Message-IDs from the headers of the messages selected for retrieval and use them to automate the generation of takedown notices if Plaintiff so desired, without any "cut and paste." If Mr. Chumura's program used the BODY command (retrieve message body without

Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

headers) instead of ARTICLE, the program could simply be changed to use ARTICLE instead[29].

70. To summarize: Defendants' requirement that those who wish to send them takedown notices under 17 U.S.C. § 512(c) refer to content by Message-IDs is reasonable and proper; Plaintiff's assertion that this requirement is "unworkable" is without merit.

I declare under penalty of perjury the foregoing is true and correct. Executed this 15th day of August, 2011.

William R. Rosenblatt

SF:316574.1

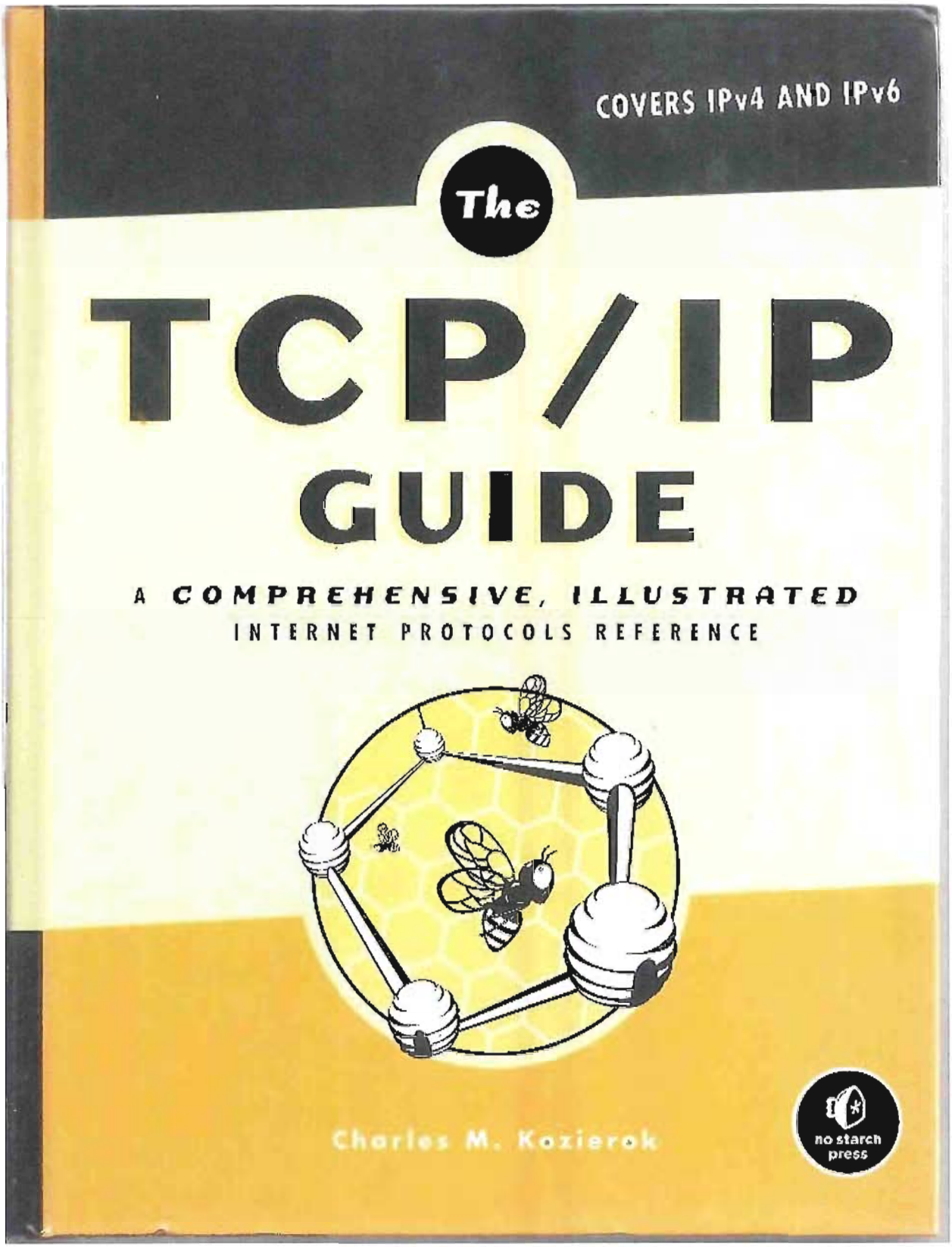
Winston & Strawn LLP
101 California Street
San Francisco, CA 94111-5802

[29] See http://tools.ietf.org/html/rfc977 Section 3.1.

TABLE OF EXHIBITS
FOR EXPERT DECLARATION OF WILLIAM R. ROSENBLATT

EXHIBIT A

Exhibit A: Description of Newsgroups



12 11 10 5 6 7 8 9 10

Printed in the United States of America

ISBN-10: 1-59327-047-X
ISBN-13: 978-1-59327-047-6

Publisher: William Pollock
Production Manager: Susan Berge
Cover and Interior Design: Octopod Studios
Developmental Editor: William Pollock
Technical Reviewers: Fernando Gont, Barry Margolin
Copyeditors: Marilyn Smith, Lisa Theobald, Mark Nigara
Compositor: Riley Hoffman
Proofreader: Stephanie Provines

For information on book distributors or translations, please contact No Starch Press, Inc. directly:

No Starch Press, Inc.
38 Ringold Street, San Francisco, CA 94103
phone: 415.863.9900; fax: 415.863.9950; info@nostarch.com; http://www.nostarch.com

Library of Congress Cataloging-in-Publication Data

Kozierok, Charles.
The TCP/IP guide : a comprehensive, illustrated Internet protocols reference / Charles Kozierok.
p. cm.
Includes index.
ISBN 1 59327 047 X
1. TCP/IP (Computer network protocol) I. Title.
TK5105.585.K69 2005
004.6'2--dc22

2004008853

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

Usenet Addressing: Newsgroups

A key concept in Usenet communication is the *newsgroup*. Newsgroups are the addressing mechanism for Usenet, and sending a Usenet article to a newsgroup is equivalent to sending email to an email address. Newsgroups are analogous to other group communication venues such as mailing lists, chat rooms, Internet Relay Chat (IRC) channels, or bulletin board system (BBS) forums (though calling a newsgroup a *list, room, channel,* or *BBS* is likely to elicit a negative reaction from Usenet old-timers!).

Like any addressing mechanism, newsgroups must be uniquely identifiable. Each newsgroup has a *newsgroup name* that describes the topic of the newsgroup and differentiates it from other newsgroups. Since there are many thousands of different newsgroups, they are arranged into sets called *hierarchies*. Each hierarchy contains a tree structure of related newsgroups.

The Usenet Newsgroup Hierarchies

The total collection of newsgroup hierarchies is in many ways similar to the domain name tree structure used in the Domain Name System (DNS). Each Usenet hierarchy is like a collection of all the domain names within a DNS top-level domain. Just as a domain name like www.pcguide.com is formed by appending the label of the top-level domain *.com* to the second-level domain name *pcguide* and the subdomain *www*, newsgroup names are created in the same way. They are created from a top-level newsgroup hierarchy name, to which are attached a set of descriptive labels that describes the newsgroup's place in the hierarchy.

One difference between DNS and Usenet hierarchies is that while DNS names are created from right to left as you go down the tree, Usenet newsgroup names are formed in the more natural (for English speakers) left-to-right order. For example, one of the main Usenet hierarchies is the *comp* hierarchy, devoted to computer topics. Within comp is a subhierarchy on data communications called *dcom*, and within that is a group that discusses data cabling. This group is called comp.dcom.cabling. Almost all newsgroups are structured in this manner.

The "Big Eight" Newsgroup Hierarchies

One problem with the decentralized nature of Usenet is ensuring coordination in certain areas where we want everyone to be on the same page, and one of these is newsgroup naming. If we let just anyone create a newsgroup, we might end up with many groups that all discuss the same topic. Imagine that someone had a question on data cabling and didn't realize that comp.dcom.cabling existed, so he created a new group called comp.datacomm.cabling. The two groups could coexist, but this would lead to both confusion and fragmenting of the pool of people interested in this topic.

To avoid problems with newsgroup creation, administrators of large Usenet systems collaborated on a system for organizing many of the more commonly used Usenet groups into eight hierarchies, and devised a specific procedure for creating new newsgroups within them. Today, these are called the *Big Eight* Usenet hierarchies, which are summarized in Table 85-1.

Table 85-1: Usenet Big Eight Newsgroup Hierarchies

Hierarchy	Description
comp.*	Newsgroups discussing computer-related topics, including hardware, software, operating systems, and techniques
humanities.*	Newsgroups discussing the humanities, such as literature and art
misc.*	Newsgroups discussing miscellaneous topics that don't fit into other Big Eight hierarchies
news.*	Newsgroups discussing Usenet itself and its administration
rec.*	Newsgroups discussing recreation topics, such as games, sports, and activities
sci.*	Science newsgroups, covering specific areas such as physics and chemistry, research topics, and so forth
soc.*	Society and social discussions, including groups on specific cultures
talk.*	Newsgroups primarily oriented around discussion and debate of current events and happenings

These eight hierarchies contain many of the most widely used groups on Usenet today. For example, professional baseball is discussed in rec.sport.baseball, Intel computers in comp.sys.intel, and Middle East politics in talk.politics.mideast.

The Big Eight hierarchies are rather tightly controlled in terms of their structure and the newsgroups they contain. The process to create a new Big Eight newsgroup is democratic and open. Anyone can propose a new group, and if there is enough support, it will be created by the cooperating system administrators who agree to follow the Big Eight system. However, this creation process is rather complex and time-consuming. Some people find this unacceptable and even object to the entire concept of this restricted process. Others consider the system advantageous, as it keeps the Big Eight hierarchies relatively orderly by slowing the rate of change to existing newsgroups and the number of new groups added.

Alt and Other Newsgroup Hierarchies

For those who prefer a more freewheeling environment and do not want to submit to the Big Eight procedures, there is an alternative Usenet hierarchy, which begins with the hierarchy name *alt*. This hierarchy includes many thousands of groups. Some are quite popular, but many are not used at all; this is a side effect of the relative ease with which an alt group can be created.

In addition to these nine hierarchies, there are dozens of additional, smaller hierarchies. Many of these are regional or even company-specific. For example, the *ne.* hierarchy contains a set of newsgroups discussing issues of relevance to New England; *fr.** covers France, and *de.** pertains to Germany. Microsoft has its own set of public newsgroups in the *microsoft.** hierarchy. Figure 85-2 shows the Big Eight hierarchies and some of the other hierarchies that exist.

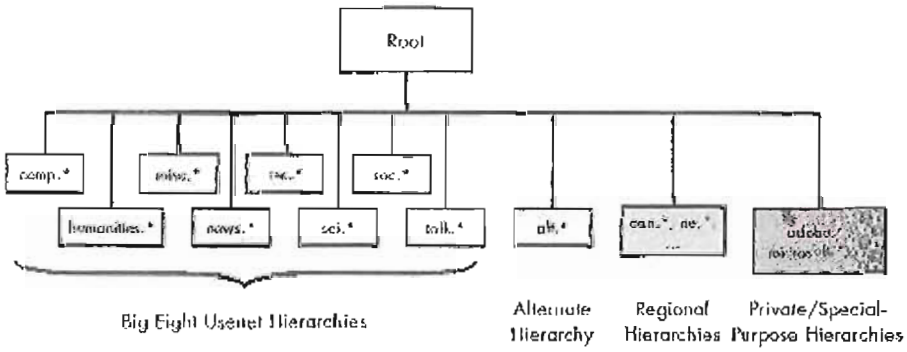


Figure 85-2: Usenet newsgroup hierarchies Usenet newsgroups are arranged into tree-like structures called hierarchies. Eight of these are centralized, widely used, general-purpose hierarchies, which are today called the Big Eight. The alternate (alt) hierarchy is a very loosely structured set of thousands of groups covering every topic imaginable. In addition to these, there are many hundreds of regional, private, and special-purpose hierarchies.

EXHIBIT B

Exhibit B: Usenet Search Results for "Zoya Konyieva"

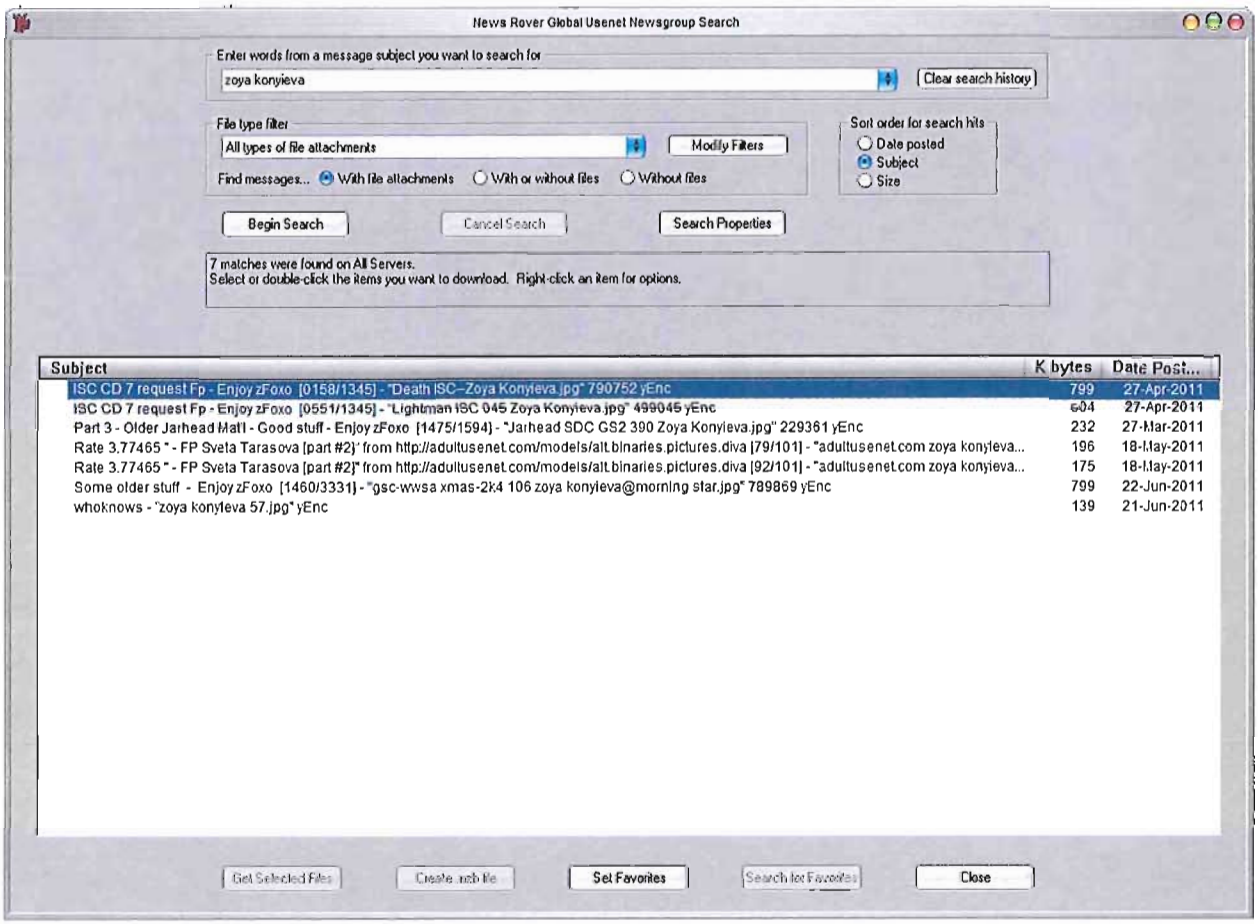


EXHIBIT C

Exhibit C: Usenet Search Results for "Ubuntu Oneiric Ocelot"

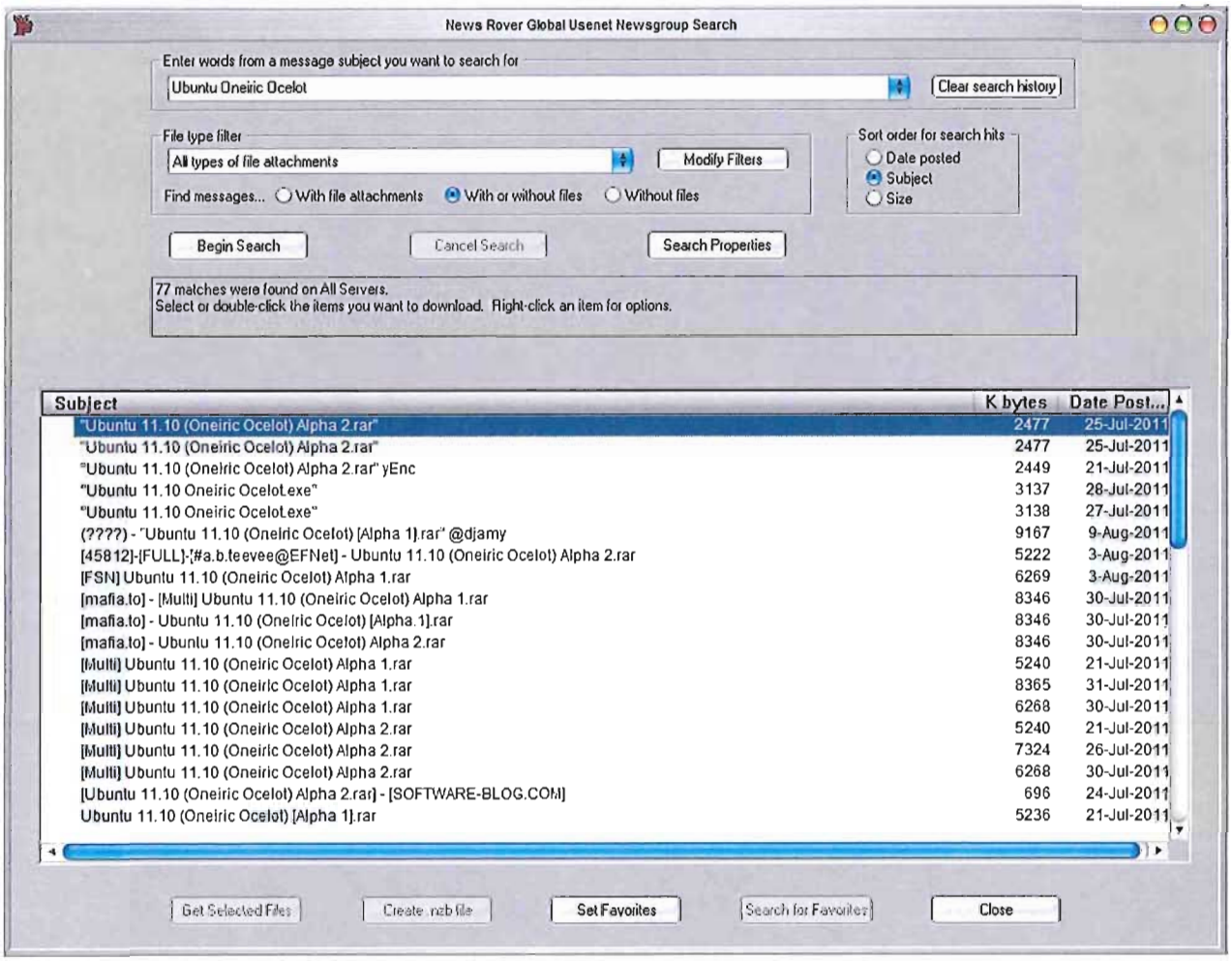


EXHIBIT D

Exhibit D: Google and Microsoft "Similar Image" Searches

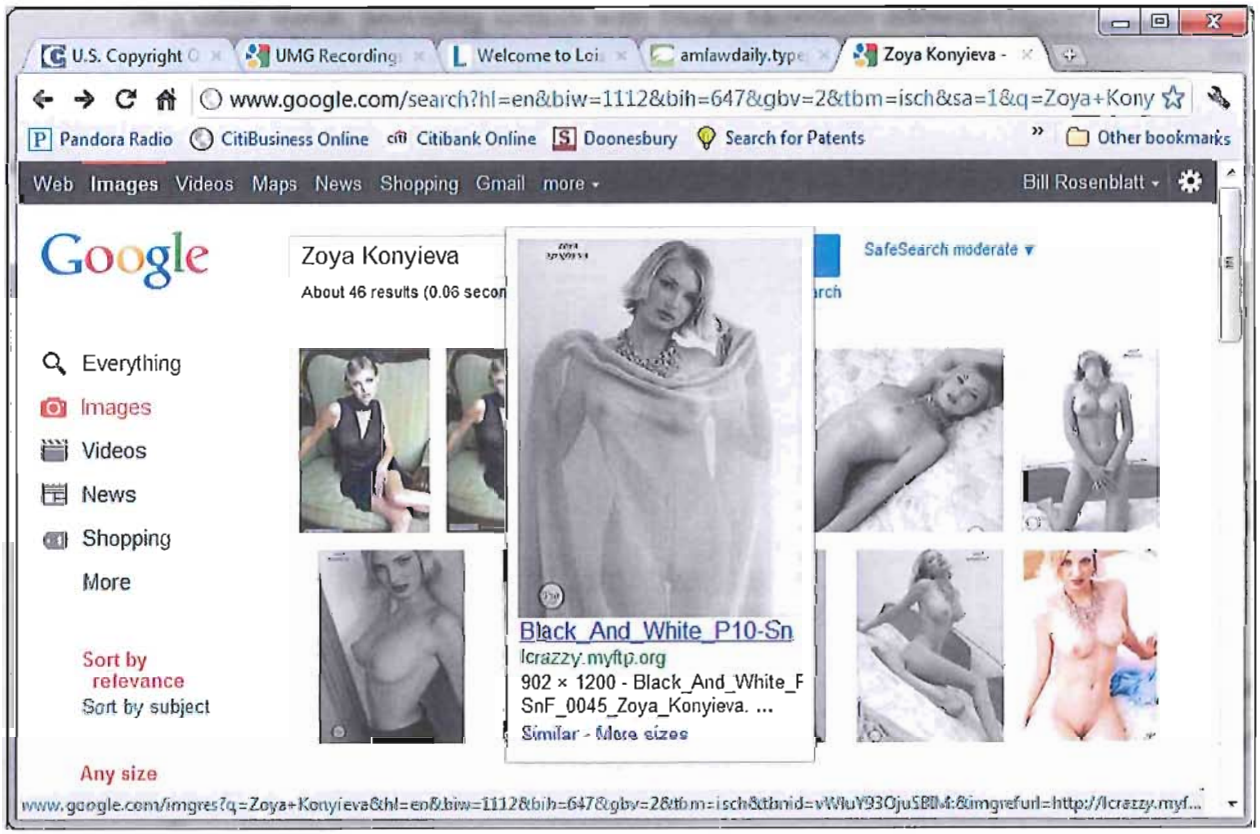


Figure 1: Google image search on "Zoya Konyieva" with mouse over one of the images.

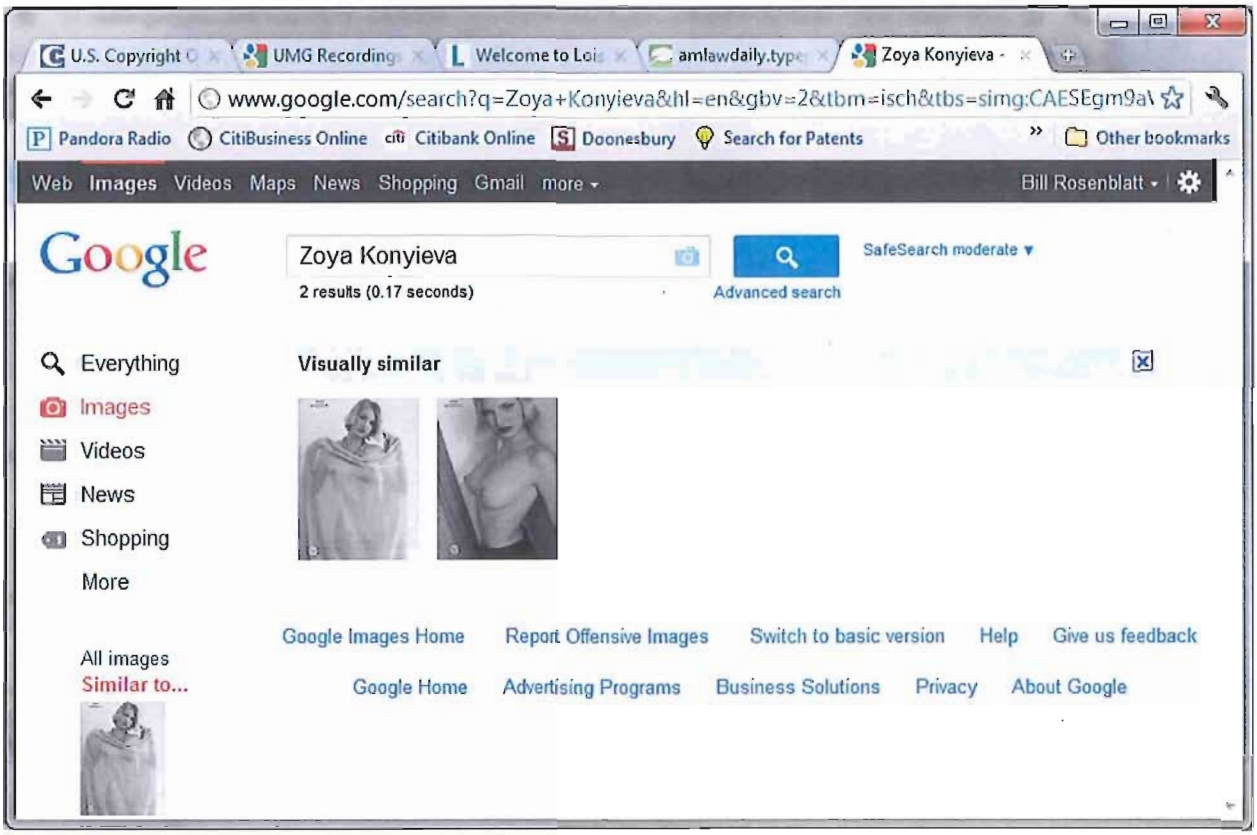


Figure 2: Google image search results after clicking "Similar" on the above search results.

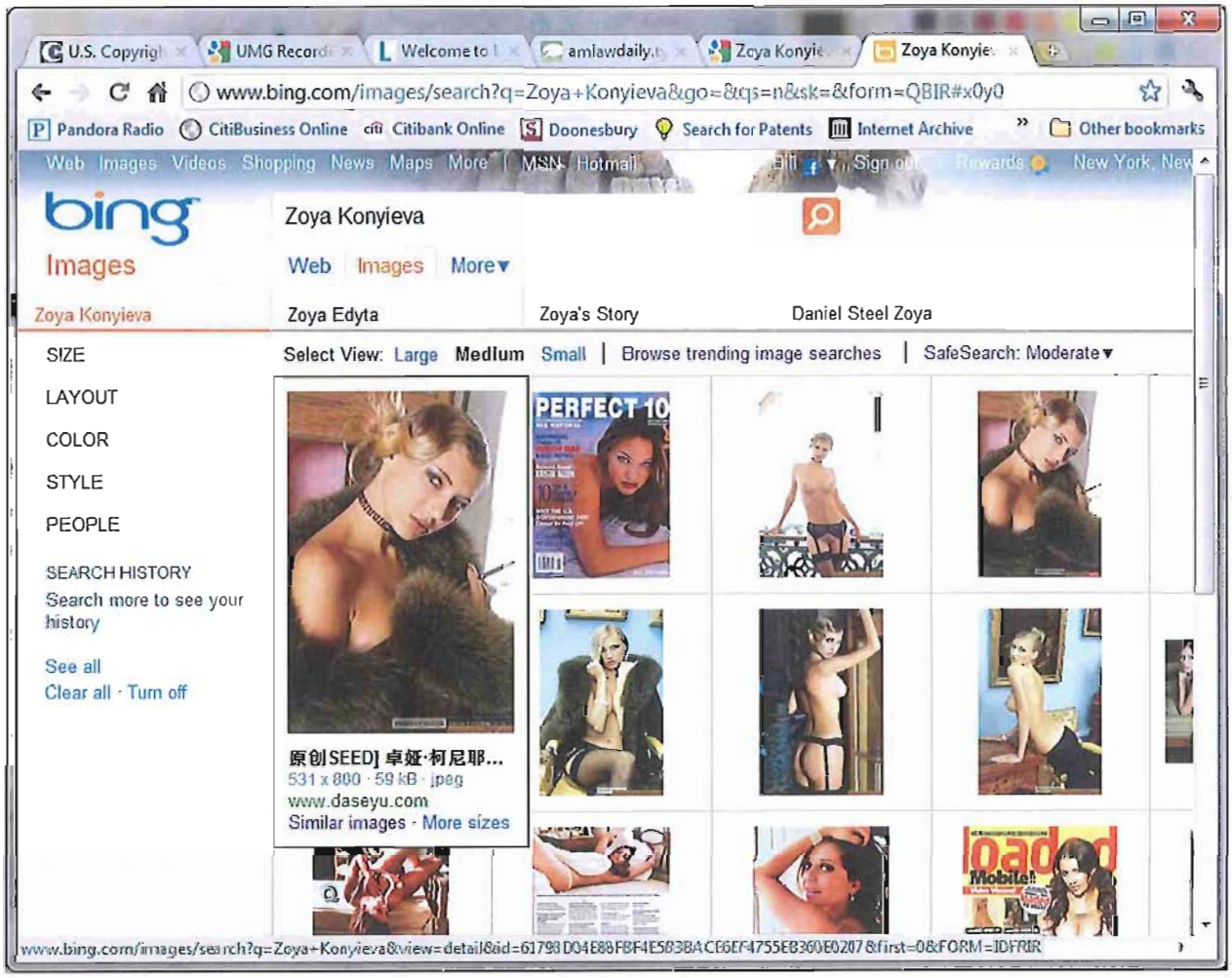


Figure 3: Microsoft Bing image search on "Zoya Konyieva" with mouse over one of the images.

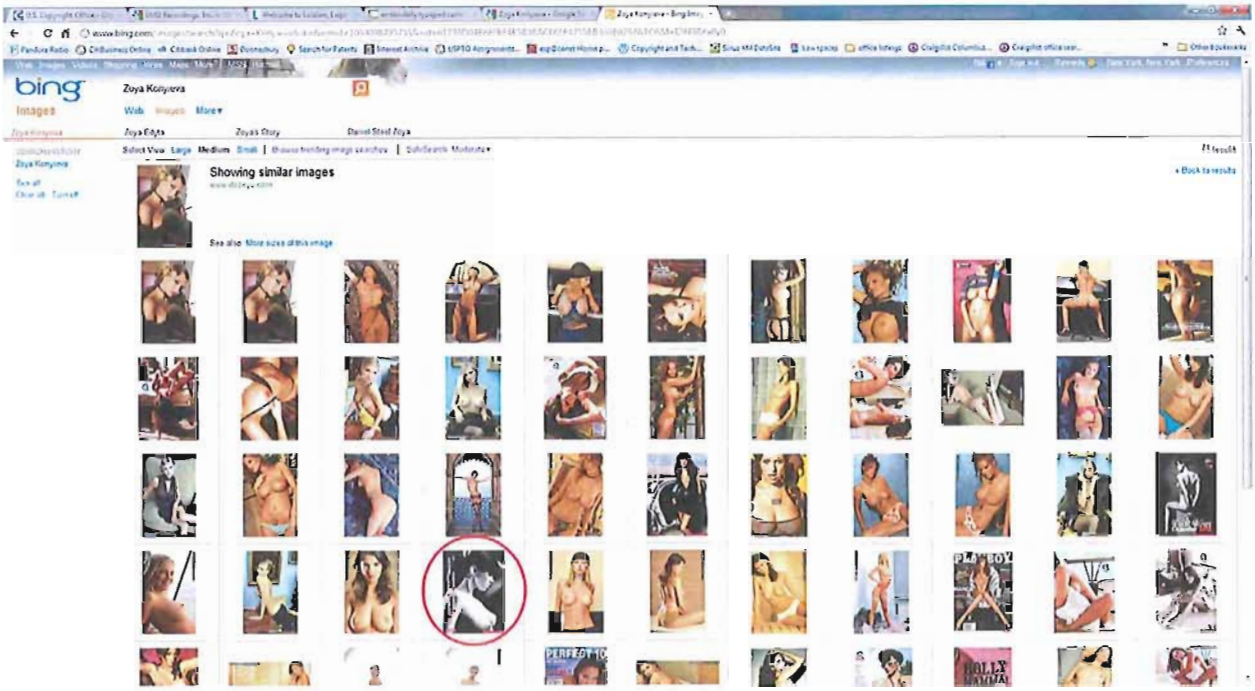


Figure 4: Microsoft Bing image search results after clicking "Similar image" on the above search results.

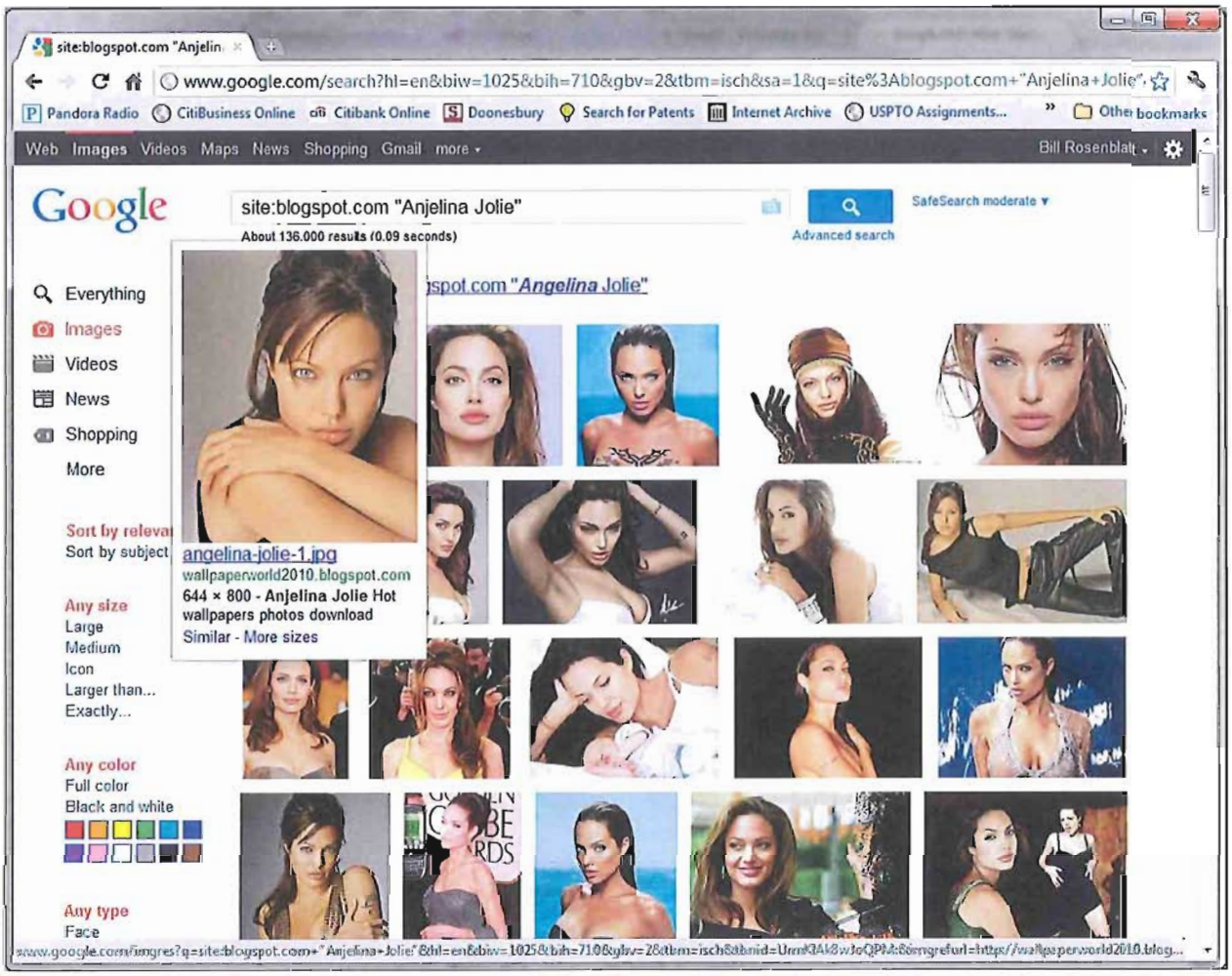


Figure 5: Google image search for "site:blogspot.com Anjelina Jolie" with mouse over one of the images.

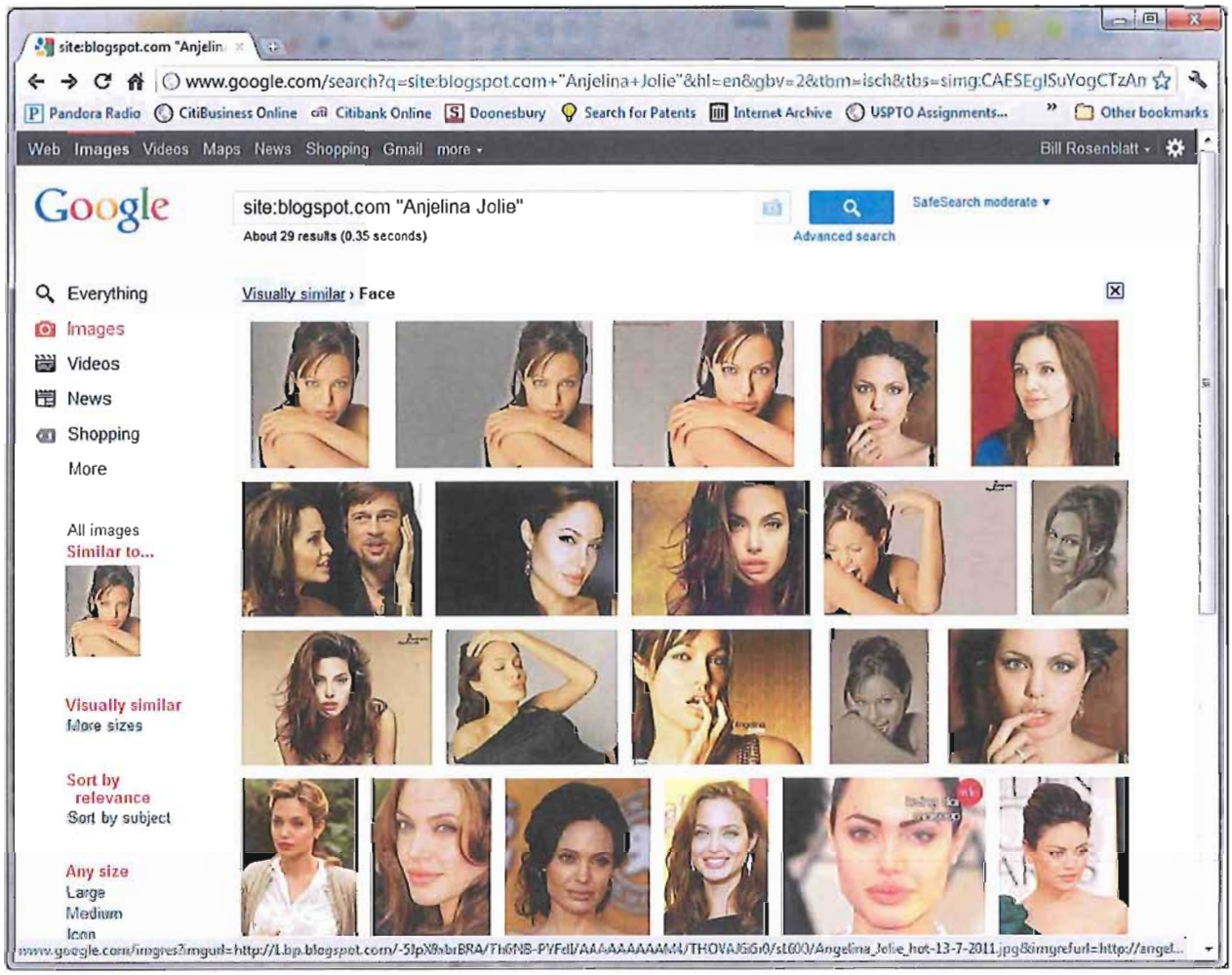


Figure 6: Google image search results after clicking "Similar" on the above search results.

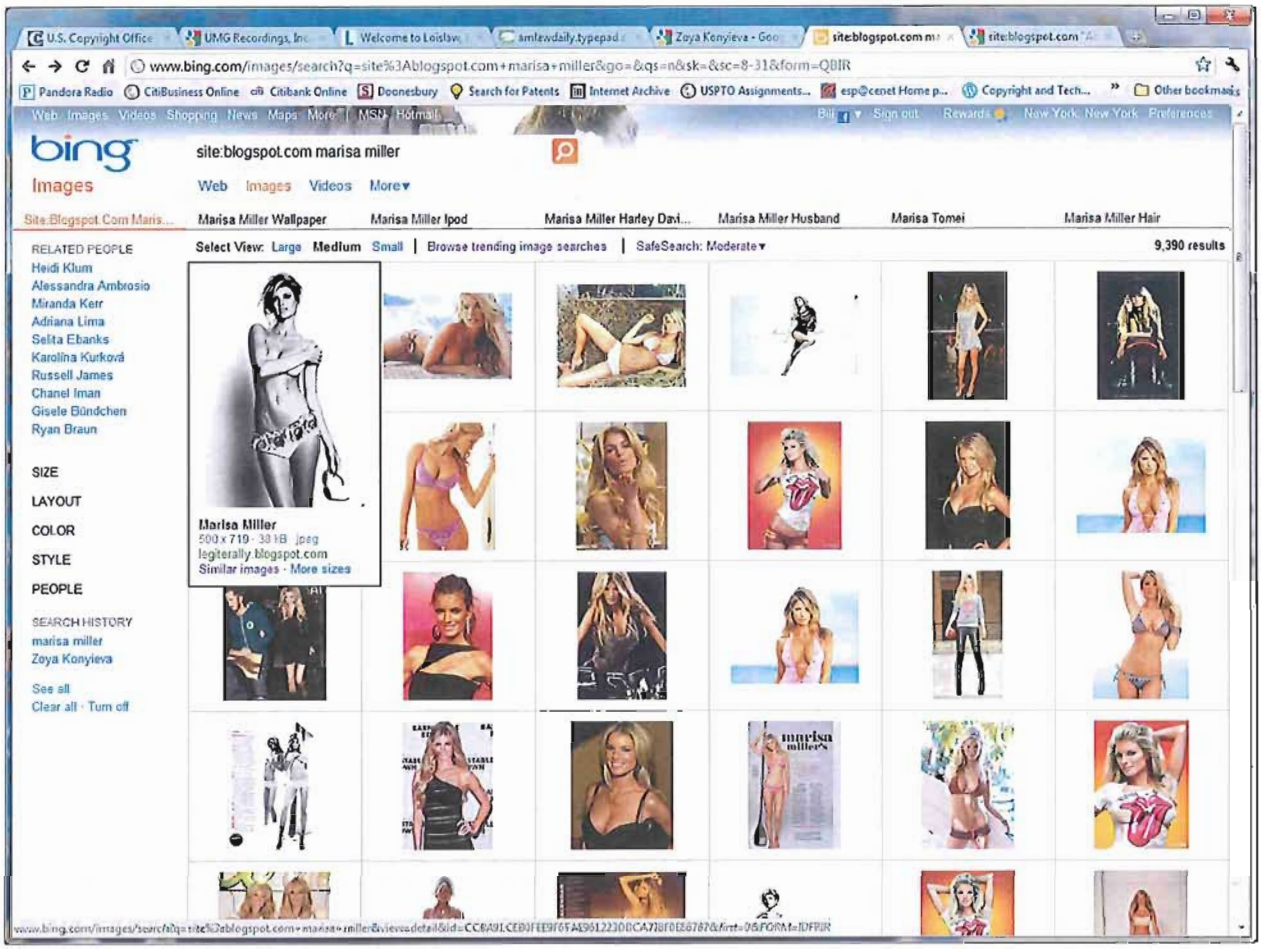


Figure 7: Microsoft Bing image search on "Marisa Miller" with mouse over one of the images.

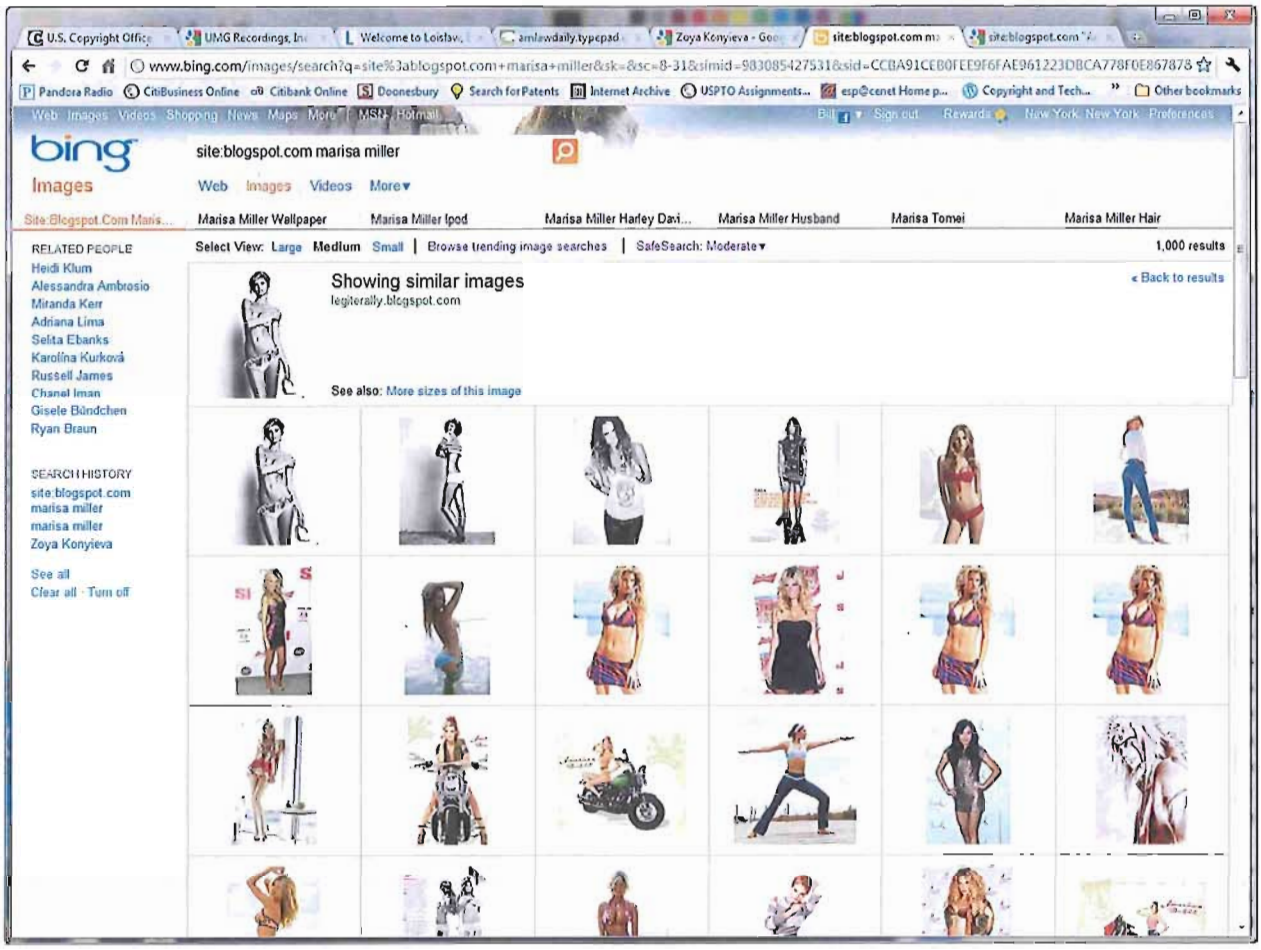


Figure 8: Microsoft Bing image search results after clicking "Similar image" on the above search results.

EXHIBIT E

Exhibit E: Usenet Search Results for "P10"

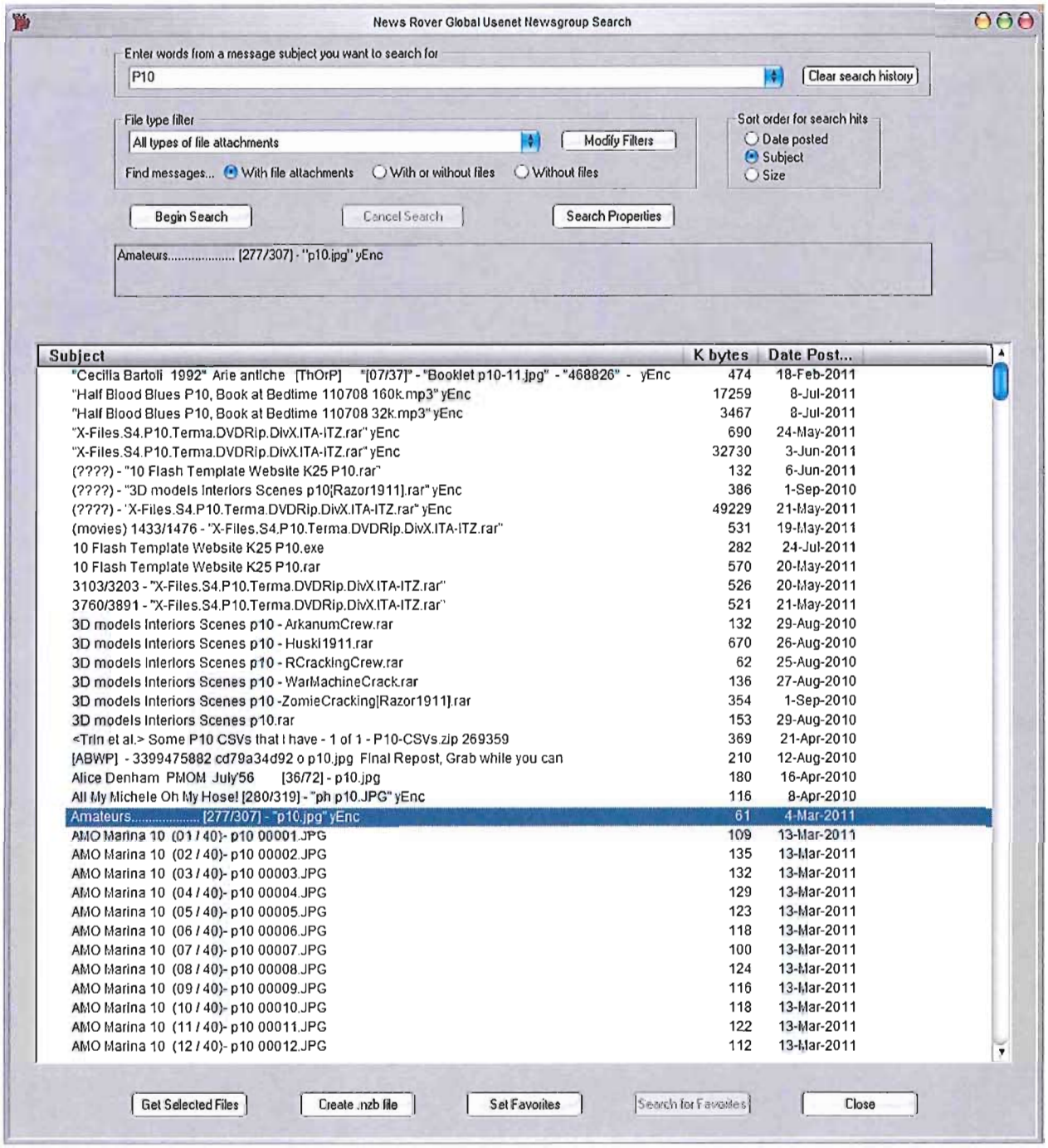


EXHIBIT F

William R. Rosenblatt

250 West 57th Street, Suite 1020
New York, NY 10107
+1 212 956 1045
Email: billr@giantstepsmts.com
Web: http://www.giantstepsmts.com/

Experience

GiantSteps Media Technology Strategies

President, June 2000 – Present.

- Management consultancy focused on the content industries. Clients include content providers and technology vendors, ranging from startups to Fortune 500 diversified media and IT companies. Services include:
  - For content providers, expertise in areas such as digital rights management (DRM), content management, digital media technologies, online content business models, and cross-media strategy.
  - For technology vendors, market strategy, business development, and product management services.
  - For public policy bodies, expertise in DRM, digital copyright, and related issues.
  - Provide expert witness and consulting services to counsel on copyright, patent, and antitrust matters regarding digital media technology, software, cryptography, and related subjects.
  - Patent litigation experience includes prior art search, infringement and invalidity analysis, claim charts, expert reports, source code discovery, testimony at deposition and trial.
- Legal support projects:
  - Served as plaintiff's technical expert witness in *Z4 Technologies v. Microsoft and Autodesk*, a patent dispute concerning software anti-piracy technology, resulting in a 9-figure jury award for willful infringement, which was upheld on appeal. Wrote two expert reports; testified at deposition and trial.
  - Served as defense technical expert in *A&M v. Napster,* a copyright dispute related to online music services. Wrote expert report.
  - Served as defense technical expert in *Digital Reg of Texas v. Hustler.com et al*, a patent dispute concerning digital video distribution, for counsel to three of the case's codefendants. Wrote three expert reports.
  - Served as technical expert in *ex parte* reexamination of U.S. Patent 5,490,216 (Uniloc); wrote two declarations under 37 C.F.R. § 1.132; participated in interviews with PTO Central Reexamination Unit examiners.
  - For counsel to a group of movie studios and an online video service, served as defense technical expert in *Intertainer v. AOL Time Warner et al*, a dispute concerning alleged misuse of confidential information related to streaming video-on-demand technology and services. Performed source code discovery; wrote expert report.
  - For counsel to a software company, served as plaintiff's technical expert in a patent dispute concerning software anti-piracy technology. Performed infringement analysis including in-depth source code discovery; created infringement contentions.
  - Served as defense technical expert in *Intertrust Technologies v. Microsoft,* a patent dispute concerning DRM technology. Provided invalidity analysis.
  - For counsel to a major music company, served as technical expert in a contract dispute concerning royalties for digital music sales. Wrote expert report.
  - For counsel to Yahoo!, served as defense technical expert in a patent dispute concerning e-commerce technology for digital music.
  - For counsel to Sharp Electronics, served as defense technical expert in a patent dispute concerning software encryption and anti-piracy technology. Provided prior art search and invalidity analysis.
  - For counsel to two major consumer Internet services, served as defense technical expert in a patent dispute concerning data distribution and licensing technology. Provided prior art search and invalidity analysis. Litigation has been stayed pending patent reexamination.
  - For a major software company, provided input to the company's response to a European Commission antitrust inquiry concerning DRM technology.
  - Provided IP portfolio monetization strategy services to several technology companies.

- Law and Public Policy:
  - Testified at the National Academies' October 2010 Workshop on Copyright Policy on Innovation in the Digital Era.
  - Testified at the Federal Trade Commission's 2009 hearings on mandatory disclosure of DRM features in digital media products and services.
  - Presented to the U.S. Copyright Office in connection with its 2003 triennial rulemaking on the anti-circumvention provision of the Digital Millennium Copyright Act (17 USC 1201(a)).
  - Presented in 2007 to the Section 108 Study Group convened by the Library of Congress on e-book licensing technologies and their effects on library storage and lending of digital works, in connection with its 5-year rulemaking on 17 USC 108.
  - Served as Special Advisor to the European Commission in connection with its Online Content in the Single Market initiative in 2007-8.
  - For a technology industry advocacy organization, contributed to an effort to educate the European Commission on issues related to copyright levies on consumer electronics.
  - For a technology industry trade association, assisted in preparing a presentation to U.S. Congress on DRM technologies and online content services.
  - Provided input to a consumer technology advocacy organization in creating a white paper on evaluating DRM technologies from the consumer's perspective.
  - For a major media company, contributed to a white paper to be used in efforts to lobby U.S. Congress for legislation on media piracy.
  - Submitted written testimony to CARP proceedings on webcasting royalties on behalf of a commercial student-run radio station.
- Sample consulting projects:
  - For a startup digital music service funded by News Corp. among others:
    - Provide competitive analysis of business models and consumer value propositions with respect to other digital music services worldwide.
    - Advise on content technologies including music metadata, music identification, and content security.
  - For a global entertainment company:
    - Helped develop a B-to-B rights management strategy, including an enterprise-wide unique asset identifier scheme, to improve the company's ability to manage and track intellectual property throughout production processes.
    - Created a survey of current DRM technologies, along with deeper technical analysis of a short list of vendor solutions and recommendations for a pilot project.
  - For a major music company:
    - Provided expertise on content security to support licensing negotiations with an online music service.
    - Performed due diligence on the company's strategic investment in R&D related to digital audio encoding technology.
  - For a global telecommunications company, created product strategy for a new type of online content service that features DRM interoperability; validated the concept through discussions with executives at leading media companies.
  - For a global consumer publisher:
    - Performed an audit of content technologies and scored them according to industry best practices. Gathered future product and new business plans and derived required technology capabilities. Created technology architecture roadmap and high-level implementation plan.
    - Created RFP for digital asset management implementation and participated in vendor selection.
  - For an online music service provider with major record label licensing, defined DRM strategy as part of technology architecture.
  - For a national newspaper, evaluated new business models and architectures for online content delivery; helped the company select a strategy and create a plan for implementation.
  - For a brand-name consumer electronics company, investigated patent acquisition opportunities in DRM, digital watermarking, and related technologies.

- For a mobile communications technology company, investigated the mobile digital broadcast market and created strategy recommendations, including promising areas for R&D and patent acquisition.
- For a global entertainment and electronics company, delivered seminars on DRM to company executives.
- For an educational and professional publishing company, gathered cross-divisional requirements for DRM for online educational materials and performed a vendor selection process.
- For a content industry trade association, organized constituents' requirements for DRM and represented it in a DRM standards working group, to ensure that the requirements were met.
- For a global information technology company, helped with product planning and design by providing expertise on how rights management should be integrated into an existing product and service based offering for the media industry.
- Provided strategic advice to several technology companies in the content security and identification markets.

- Client list and further sample project descriptions available on Web site www.giantstepsmts.com. Further details about clients and projects available on request.

DRM Watch/Copyright and Technology
Editor and Publisher, 2001 – 2003.
Managing Editor, 2003 – present.

- The leading e-newsletter on digital rights management, featuring analysis of DRM-related news events, white papers, and other resources. Founded www.drmwatch.com in September 2001, sold to Jupitermedia Corp. in October 2003. Repositioned as the blog Copyright and Technology (copyrightandtechnology.com) in January 2009.

Conference Programming
Jupiter DRM Strategies Conference, 2004 – 2007.
Gilbane Enterprise DRM Conference, 2006.
Copyright and Technology Conference, 2010.

- Program chair of conferences devoted to digital copyright and rights technologies.
  - April 2004, New York City
  - November 2004, Los Angeles
  - July 2005, New York City
  - April 2006, San Francisco
  - November 2006, Boston
  - September 2007, New York City
  - June 2010, New York City

Morningside Ventures Inc./Fathom
Chief Technology Officer, August 1999 – June 2000.

- CTO of Morningside Ventures, Columbia University's internet business incubator.
- Led technical implementation of Fathom.com, a Morningside Ventures spinoff. Fathom.com was a destination website for authenticated knowledge and e-commerce sponsored by Columbia, the London School of Economics, Cambridge University Press, the New York Public Library, the Smithsonian, and other educational and cultural institutions. Responsibilities included technology architecture, selection of and negotiation with technology partners, web hosting, e-commerce outsourcing, and internal IT management. Managed internal staff and various vendor relationships.

The McGraw-Hill Companies
Vice President, Technology and New Media, March-August 1999.

- CIO for McGraw-Hill's vertical trade publishing division. Responsible for front and back office IT, including desktop publishing and mainframe environments. Managed department of 30 people.
- Defined technology strategy for B-to-B vertical market web portals, including AviationNow.com, an information portal for the aviation industry.

- Architected intranet front end to legacy customer service system for all McGraw-Hill magazines.
- Internal consultant on cross-divisional content management architecture.

Sun Microsystems
Market Development Manager, Media & Publishing, 1997-1999.

- Set market strategy for Sun in publishing industry, focusing on content management, DRM, web technologies for publishers, and newspaper systems. Drove strategy through sales force.
- Recruited and managed alliances with software vendors and other partners, including Vignette Corp. and Quark, Inc.; executed joint marketing agreements. Drove over $20 Million revenue through partner investments.
- Consultant to media industry customers. Example projects: content management and online delivery for educational publisher; online rights management for scientific publisher.
- Author of whitepapers and articles; maintainer of Sun's media industry web site.
- Organized and produced Technology Workshop around the DOI standard (see below); attracted about 30 technology vendors.

Enterprise IT Architect, 1996-1997.

- Technology consultant to media industry customers. Example projects: enterprise content management architecture for trade periodical publisher; next-generation editorial system strategy for consumer magazine division of diversified media company; digital asset management strategy for major film studio.
- Did business development for Sun MediaCenter streaming media server product line.
- Developed Sun's Digital Media Management solutions strategy & reference architecture.
- Built Sun Digital Media Solutions Center in New York City.

The Times Mirror Company
Director, Publishing Systems, 1994-1996.

- Leader of Times Mirror Digital Library initiative, family of digital content management projects across Times Mirror book, newspaper, and professional information companies involving distributed editorial libraries for newspapers; mass-customized textbook publishing; editorial process reengineering; intellectual property management and control.
- Managed project budgets totaling over $16 Million.
- Technology consultant to Times Mirror operating units and Corporate Strategic Development. Projects included MDConsult.com, a web service for physicians; online aircraft maintenance documentation, custom publishing of professional training materials; evaluation of search technology company for potential acquisition.
- Company representative on industry committee that led to definition of Digital Object Identifier (DOI) standard for Digital Rights Management, which is gaining acceptance among book and journal publishers internationally. Was one of the designers of the DOI.

Moody's Investors Service
Manager, Information Resources, 1992-94.

- Responsibilities included emerging technologies R&D and software quality assurance.
- Architect of electronic publishing service based on Lotus Notes, Adobe Acrobat, and Sybase.
- Led global Lotus Notes rollout.
- Introduced technologies to company: groupware, expert systems, automated software testing.
- Promoted from Technical Consultant position.

The Rustin Group
Senior Software Developer, 1991-92.

- Developed sales tracking system for international barter company.
- Managed benchmark of production system for financial information publishing division of Citicorp on Unix-based multiprocessor computers.
- Began software product initiatives in software development tools and computer music composition.
- Established and managed college recruiting program.

University of Massachusetts
Research Assistant, 1986-91.
- Conducted doctoral research in software engineering, object-oriented languages, and database technology as part of ARCADIA multi-institutional research consortium.
- Built several prototype software engineering tools in C, C++, Lisp, and Ada.
- Published research papers (list available on request).

Instructor, 1990.
- Taught CS520, senior and graduate-level course in software engineering.

Intermetrics, Inc.
Software Engineer, Electronic Systems Group, 1985-86.
- Manager of UNIX data center, system administrator, and software tool developer (C, Lisp).
- Gave tutorials on UNIX topics (system administration, internals, shell programming, etc.).
- Developed software for Free Software Foundation's GNU Emacs editor project.

Motorola Information Systems Group
Software Engineer, Computer Services Group, 1984-85.
- System administrator and software tool developer (C and Shell languages) for network of UNIX super-microcomputers.
- Served as company-wide authority on UNIX; gave tutorials on UNIX-related topics.
- Tools developed included shared-memory batch queue for UNIX System V, editor-like interface to UNIX Shell, cross-assembler (on Apollo workstation) for custom VLSI signal processing chip.

Associate Engineer, Modulation Products, 1983-84.
- Project team member for 2600 series of high-speed modems based on Motorola 68000 microprocessor. Implemented network control interface; designed and implemented remote datascope feature (68000 assembly language).

Freelance Writer & Editor
1991-present.
- Editor, *Copyright and Technology* (copyrightandtechnology.com); see above.
- Managing Editor, *DRM Watch* (www.drmwatch.com); see above.
- Author, *Digital Rights Management: Business and Technology* (John Wiley & Sons, 2001).
- Author, Digital Rights and Digital Television, chapter in *Television Goes Digital* (Springer, 2009).
- Author of white papers on DRM and content management.
- Editor of Harris Kern, *Discipline: Six Steps to Unleashing Your Hidden Potential* (FirstBooks, 2001)
- Author and editor of books on UNIX and Java related topics (O'Reilly & Associates).
- Contributing Editor of IDG's *Advanced Systems*, *SunWorld*, and *Unix Insider*.
- Author of articles in *Salon, The Seybold Report, eContent, INDICARE Monitor,* and other periodicals.
- Full publications list available on Web site at www.giantstepsmts.com/publications.htm.

Guest Lectures
- Columbia University
- Rutgers University School of Law
- New York University School of Law
- University of Maryland Center for Intellectual Property
- Franklin Pierce Law Center
- Drexel University
- New York City College of Technology

Education
- B.S.E. (*cum laude*) in Electrical Engineering and Computer Science, Princeton University, 1983.
- M.S. in Computer Science, University of Massachusetts, 1990.

- Coursework for Ph.D. in Computer Science, University of Massachusetts; dissertation topic: *Specification Level Interoperability in Software Development Environments.*
- Executive education: Harvard and University of Southern California business schools.
- Language skills: proficient in German.

Affiliations

- Advisory trustee and former board chairman, Princeton Broadcasting Service, Inc., corporation overseeing WPRB-FM and *The Nassau Weekly* newspaper, Princeton, NJ.

Interests

- Cooking
- Cycling
- Collecting Sherlock Holmes pastiche fiction
- Rock music history